4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/779,613	02/09/2001	Maurice Ostroff	1294	5742

7590 06/22/2004

Edward Langer
Landon & Stark Associates Ltd.
One Crystal Park Suite 210
2011 Crystal Drive
Arlington, VA 22202

EXAMINER	
LE, DAVID Q	
ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 06/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/779,613	**Applicant(s)** OSTROFF, MAURICE	
	Examiner David Q Le	**Art Unit** 3621	MW

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 February 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. The Examiner has pointed out particular references contained in the prior art of record in the body of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures apply as well. It is requested from the Applicant, in preparing the response, to consider fully the entire references as well as the context of all passages in the cited references as potentially teaching all or part of the claimed inventions.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

3. **Claims 1, 7-8, and 10-22** are rejected under 35 U.S.C. 102(a) as being anticipated by ***Flitcroft et al.***, US Patent Application Publication No. US 2003/0028481 A1.

As per **claims 1, 20 and 22**.

Flitcroft discloses

A method [claims 1, 20] and system [claim 22]

for preventing fraudulent card transactions in systems such as card payment and card access systems (Abstract; Object and Summary of the Invention),

online [claim 1] and off line [claim 1, 20] ,

while performing an offline [claim 20] or computer/other device [claims 1, 22] card transaction, said transaction typically associated with at least one activity performed by a user in transacting with a vendor, said vendor being a person, an entity, a computer or a machine and wherein said at least one activity is performed by the user from among a group of activities relating to acquiring of goods or services, and/or access to a computer, a network and/or virtual and physical sites, (Abstract; Background, Objects and Summary of the Invention) said method comprising:

providing the user with a physical card by a card issuer (above, following citations),

said card being embodied in a portable, digitally recordable medium having stored thereon a user program [claims 1, 22] that does not require storage of any component of said user program on a computer, (Paragraphs #72; #327: "smart cards"; Figs 1, 5, 6; associated text);

said card being embodied in a non-digital portable medium [claim 20] (Par 49, 72: "card numbers can be printed on a form 136 by printer 130, which is then delivered to the customer via the mail"; Fig 1; associated text);

allocating to said physical card a unique identification number (ID), a password, and where applicable, an account number (Par 74; 119, Fig 2, 5, 6; associated text);

recording in a database associated with the card issuer for each card so provided, details of said ID and said password together with details of the user to whom the card has been provided (Par 70; Fig 1-2; 5-6; associated text);

initiating the card transaction in one of offline (see all above citations; Par 283-302) and online modes (see all above citations; Par 117-130),

wherein during said offline mode, said card transaction is initiated by: communicating a Cybercoupon (all above citations; Par 56-57: "Controlled Payment Number, or CPN"; "limited use credit card numbers") as part of said card transaction, to the vendor in any manner not involving online communications,

and wherein during said online mode, said card transaction is initiated by: connecting the computer online; communicating a Cybercoupon as part of said card transaction, to the vendor via online communications (see all above citations);

receiving said Cybercoupon at the vendor, and processing said card transaction by the vendor; transmitting by the vendor to the card issuer via a communication network, a request for authorization of the card transaction, if the vendor requires authorization by the card issuer before said vendor is entitled to give effect to said transaction; receiving said request for authorization at the card issuer; processing, by the card issuer of said request for authorization in accordance with its standard criteria; authorizing the card transaction, if said Cybercoupon is determined to be valid and if the card issuer's standard criteria are met; or otherwise rejecting the card transaction (Figs 7-8; associated text);

[claim 20]

allocating said card a quantity of Cybercodes listed in a predetermined sequence and in which an indicator in said ID indicates that said ID is invalid unless it has been modified by said Cybercode and wherein, the user selects one Cybercode at a time in accordance with said sequence and uses said Cybercode to create a Cybercoupon comprising said ID modified by the addition of said Cybercode as an extension to said ID or by inserting said Cybercode in said ID in replacement of the equivalent number of digits in a predetermined position of said ID, said Cybercoupon being used in lieu of the user's regular card number when initiating a card transaction (Par 70, 71, 74, 75, Fig 2; associated text);

[claim 20]

..receiving said request for authorization at the card issuer; and

authorizing the card transaction, in accordance with an authorization method comprising:

receiving of said request initially by a Filter Program (Fig 7; 8; steps 710 and 810; associated text) at the card issuer; differentiating by said Filter Program between requests containing Cybercoupons generated by said added Cybercode method and requests containing other card numbers (same as above);

directing by said Filter Program of a request which does not contain said Cybercoupon to the card issuer's standard processing system; forwarding a request which contains said Cybercoupon to a Translator Program associated with said Filter Program; detecting by paid Translator Program of the ID contained in a request containing a Cybercoupon and by reference to said database at the card issuer linking said ID with the relevant account number associated with said ID (Fig 7, 8; associated text);

checking whether said Cybercode has been used previously in association with said ID and if so rejecting the relevant request; marking, if said Cybercode has not been previously used, said Cybercode as having been now used (Fig 7, 8; associated text; Par 76; Par 185-189),

comparing the data stored in said database to ensure that said Cybercode is in the correct position in the predetermined sequence; determining that information contained in said request for authorization received from said vendor matches the information contained in said notification received from said user; rejecting a request which fails any of said checks and notifying said vendor accordingly; substituting, in a request which has passed all checks, the relevant account number for said Cybercoupon and transmitting said request with said substituted account number, to the card issuer's standard processing system; retaining a record of all incoming requests which contained Cybercoupons and said relevant permanent account numbers which have been passed to the card issuer's standard processing system; processing of said request for authorization by the card issuer's standard processing system in accordance with its standard criteria (Fig 7, 8; associated text; Par 185-189);

responding by said card issuer's said standard processing system to said Filter Program that said request has been rejected if said criteria have not been met; responding by said card issuer's said standard processing system to said Filter Program that said request has been accepted if said criteria have been met, forwarding by the Filter Program to the vendor of said response with the card number unaltered if the original request did not contain a Cybercoupon; forwarding by the Filter Program to said Translator program of said response, if said response relates to a request that contained a Cybercoupon when received; replacing, by said Translator Program of said permanent card number with said original Cybercoupon in respect of a request which was originally received containing a Cybercoupon; transmitting said response containing said Cybercoupon by said Translator Program to the vendor; and transmitting said response to the user (Fig 7, 8; associated text; Par 185-189).

As per **claim 7**.
Flitcroft further discloses all the limitations of this claim (see all above citations):
... said card contains a quantity of Cybercodes...;
maintaining at the card issuer, a database ...;
inserting said physical card in the computer ...;
entering said password ...;
selecting by said program of the next unused Cybercode ...;
generating a Cybercoupon ...;
communicating, in an offline transaction, said Cybercoupon to the vendor...;
entering, in an online transaction, said Cybercoupon in a vendor's order form ...;
interacting, ...of said user program with said user's email program or browser ...;
receiving by said card issuer ...;
receiving said order by said vendor ....

As per **claim 8**.
Flitcroft further discloses all the limitations of this claim (see all above citations):
...the vendor's right to give effect to said card transaction ...
transmitting details of the proposed transaction ...;
receiving of said request ...;
differentiating by said Filter Program ...;
directing by said Filter Program of a request ...;
detecting by said Translator Program of the ID ...;
checking by said Translator Program ...;

substituting, ... said account number for said Cybercoupon, ...;
checking whether said Cybercode has been used previously ...;
marking, ... said Cybercode as having been now used;
comparing the data stored in said database ...,
comparing that information ...matches the information ... from said user;
rejecting a request which fails any of said checks ...;
substituting, ...the relevant account number...;
retaining a record of all incoming requests ...,
processing of said request for authorization ...;
responding by said card issuer's ...;
replacing, by said Translator Program ...;
transmitting said response ... to the vendor;
transmitting said response to the user.

As per **claims 10-14**.

Flitcroft further discloses all the limitations of these claims (see all above citations):

[claim 10] ... the card contains a store for storage of encryption keys and a commonly available encryption algorithm for encrypting a Cybercoupon for use as a password in the form of a challenge, ... in accordance with a method comprising:

requesting by the user of permission to logon to a server; responding by said server with a challenge; extracting by said user program of a key from said store; generating a Cybercoupon by using said key in conjunction with said algorithm to encrypt said challenge; transmitting said Cybercoupon together with the card ID to the server; using the ID by the server to identify the key; using said key to decrypt said Cybercoupon; comparing the decrypted Cybercoupon with the original challenge; and authenticating the user if said response is identical to said challenge.

[claim 11] ... using asymmetric keys.

[claim 12] ... the card contains a store for storage of encryption keys and a commonly available encryption algorithm for encrypting text which encrypted text can be stored securely on a local or remote computer or transmitted as a message electronically.

[claim 13] ... said user program interacts with the user's email program to generate secure encrypted messages by email.

[claim 14] ... said card takes the form of a combined magnetic stripe card and a smartcard in one unit, enabling said user to choose to use said card either as a conventional magnetic card or as a smartcard, said combined card containing a conventional magnetic stripe and any one of said user program described herein for generating Cybercoupons or passwords.

As per **claim 15-18**.

Flitcroft does not specifically recite all the limitations of these claims. However he does teach that his system will be able to use audible tones to transmit and process the limited use credit/debit card numbers and transaction information for the purpose of authorizing said transactions (Par 127; all above citations); therefore all of the following claimed limitations would have inherently been included features in Flitcroft's system:

[claim 15] ... said card contains a Dual Tone Multifrequency (DTMF) Generator in addition to said user program which interacts therewith in accordance with a conversion method so as to convert said Cybercoupon to an audio tone Cybercoupon, each digit in said Cybercoupon being converted to a specific audio frequency in accordance with international telephony standards, said conversion method comprising: inserting said card in a computer; generating a Cybercoupon; converting said Cybercoupon to an audio signal; and transmitting said Cybercoupon to the vendor directly modem tó modem.

[claim 16] ... said card contains a Dual Tone Multifrequency (DTMF) Generator in addition to said user program which interacts therewith in accordance with a conversion method so as to convert said Cybercoupon to an audio tone Cybercoupon, each digit in said Cybercoupon being converted to a specific audio frequency in accordance with international telephony standards, said conversion method comprising: generating a request for permission to logon to a server; converting said request to an audio signal recognizable by said server; transmitting said audio signal to the server; responding by said server with an audio challenge; converting said audio challenge to text; extracting by said user program of an encryption key from said store; using said encryption key to generate a Cybercoupon comprising said challenge encrypted using said algorithm; converting said Cybercoupon to an audio tone Cybercoupon and converting said ID to an audio signal; transmitting said audio tone Cybercoupon in response together with the audio card ID to the server; using the ID by the server to identify said encryption key; using said encryption key to decrypt said Cybercoupon; comparing the decrypted response with the original challenge; authenticating the user if said response is identical to said challenge. transmitting said audio tone Cybercode to the vendor.

[claim 17] said DTMF card is self-contained and operates without the use of a separate computer, said DTMF card including a keypad, a speaker and optionally a screen in addition to said user program and said DTMF generator, thus enabling a Cybercoupon to be generated, converted into audio tones and transmitted by placing the speaker on the card close to the microphone of the telephone or other means of audio communication.

[claim 18] said DTMF-card is used in association with a telephone calling card provided by a telephony service provider, said Cybercoupon comprising the user's ID and PIN encrypted and converted to audio signals as described.

As per **claim 19**.

Flitcroft further discloses (see all above citations):

... a POS Module is provided at an outlet equipped with commercial Point of Sale (POS) software, said module being designed to interact with said outlet's POS software enabling said POS Module to activate said card, read said Cybercoupon generated by said card and treat said Cybercoupon as a regular card number for processing in the usual manner adopted by said outlet.

As per **claim 21**.

Flitcroft discloses all the limitations of this claim (see all above citations):

...the user is supplied with a unique supplementary code to be used in conjunction with each said Cybercode so that an unauthorized person who obtains access to said list of Cybercodes is unable to use said Cybercodes without knowledge of said supplementary code.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 2-4 and 9** are rejected under 35 U.S.C. 103(a) as being unpatentable over ***Flitcroft***.

As per **claim 2**.

Flitcroft further discloses

... after connecting the computer online, and after downloading a vendor's order form, inserting, when a card number is required for the purpose of the transaction, said card in the computer and activating said user program (Fig 6; associated text; Par 117-130), entering the password to gain access to said user program (same as above); generating said Cybercoupon (Par 119); displaying, in optional fashion, advertising material contained in said user program (Par 239, 241); and inserting said Cybercoupon on said order form in the position requiring a card number (Par 127).

Flitcroft does not recite

..online intrusion during online card transaction is minimized by ...disconnecting automatically said card from the computer by ejecting the relevant drive or by other means.

However Flitcroft teaches the use of card-swipe readers in his system (Fig 1; Par 69). These readers would not retain the cards and therefore would minimize any possible "online intrusion". Similarly, it would have been obvious to one ordinarily skilled in the art at the time the invention was made to provide for mechanisms to release the cards once a reading is made, in order to (1) return it to the user and (2) to minimize risk for online intrusion.

As per **claim 3**:

Flitcroft further discloses

inserting, when a card number is required for the purpose of the transaction, said card in the computer and activating said user program (Fig 6; associated text; Par 117-130); entering the password to gain access to said user program; generating said Cybercoupon; displaying, in optional fashion, advertising material contained in said user program (Par 239, 241); connecting the computer online and downloading a vendor's order form; inserting said Cybercoupon on said order form in the position requiring a card number (Par 117-130).

Flitcroft does not recite

..online intrusion during the card transaction is avoided during said online mode, by disconnecting said card from the computer by ejecting the relevant drive or by other means.

However Flitcroft teaches the use of card-swipe readers in his system (Fig 1; Par 69). These readers would not retain the cards and therefore would minimize any possible "online intrusion". Similarly, it would have been obvious to one ordinarily skilled in the art at the time the invention was made to provide for mechanisms to release the cards once a reading is made, in order to (1) return it to the user and (2) to minimize risk for online intrusion.

As per **claim 4**.

Flitcroft does not disclose

... said password may comprise at least a single word and wherein said user program is designed so that if an incorrect password is entered more than a predetermined number of times, the user gains entry to said user program and a fictitious Cybercoupon is generated having the appearance of a regular Cybercoupon but containing a code which indicates to the card issuer, that an irregular attempt has been made to enter the password, thus enabling the card issuer to take such steps as it considers appropriate.

However Flitcroft does teach a method for thwarting fraudulent, brute force attempts to guess a credit/debit card's password: "A consecutive number of errors in inputting the password will permanently disable the program and overwrite remaining encrypted numbers" (Par 148). Also it is well known in the industry that credit/debit card issuers often monitor the usage patterns of the cards issued to their customers and are quick to alert their customers if unusual card activity is detected. It would have been obvious to one ordinarily skilled in the art to combine Flitcroft's security measures with those customarily used in the industry to issue specially tagged Cybercoupons in instances of fraudulent card use, so that card issuers may take steps to either alert the card users or take any further steps as they may consider appropriate.

As per **claim 9**.

Flitcroft does not recite

... said processing procedure contains a calculating means for statistically determining an acceptable tolerance in variation from said predetermined sequence of said Cybercode, taking into account such factors as the norm for the particular industry between the time and date on which a vendor receives an order and the time and date on which a Card Issuer receives the relevant request for validation from said vendor, and the value of the order, so that a transaction quoting an out of sequence Cybercode will be authorized with a statistically calculated level of safety, provided that such Cybercode falls within said calculated tolerance.

However he does teach many methods which may be used to generate limited use credit/debit card numbers (the claimed Cybercodes) so that statistically there will be no risk of using them and/or authorizing them in out of sequence situations (see all above citations; Par 80-98). Therefore it would have been obvious to one ordinarily skilled in the art to have added one more method as described in claim 9 in order to ensure that Cybercodes may be authorized out of sequence when they statistically fall within industry accepted standards for the times between user report of their use and merchant request for their authorization. Such an added method would make the system more flexible and would cause less false rejections of otherwise legitimate authorization requests, thus making the system more attractive to consumers and merchants alike.

6. **Claims 5 and 6** are rejected under 35 U.S.C. 103(a) as being unpatentable over ***Flitcroft*** as applied to claim 1 above, and further in view of ***Franklin et al.***, US Patent No 6,000,832.

As per **claim 5**.

Flitcroft further discloses

said user program stored on said physical card [uses] a one-time Cybercoupon in encrypted form, emulating a regular card number and containing encrypted information relating to the card ID and, where applicable, the monetary value of the transaction, the vendor identity and other information relating to the card transaction and wherein said processing by the card issuer includes decrypting said Cybercoupon, in a method comprising (Fig 6, associated text; Par 117-130): inserting said physical card in the computer and activating said card so as to display a login window on the computer screen; entering said password in said login window so as to activate said encryption program which opens a dialog box on the screen; entering where applicable, the currency and monetary value of the card transaction and the vendor's identity in relevant positions in said dialog box (same citations as above);

displaying said encrypted Cybercoupon on a screen; communicating, in an offline transaction, said Cybercoupon to the vendor, in any manner not involving online communication (Par 127); entering, in an online transaction, said Cybercoupon in said order form and communicating said order form to the vendor online; and receiving said order form by the vendor and processing said transaction in accordance with its usual procedures (same citations as above).

Flitcroft does not disclose that

..said user program on said physical card comprises a number generator and an encryption program, which, on receiving the appropriate command, generates said one-time Cybercoupon. Rather, Flitcroft discloses that the limited use credit card numbers of his system (the claimed Cybercodes) will be generated randomly by the card issuer's central server, using a random number generator (Fig 2, associated text; Par 74, 81-82, 88), and then provided to the debit/credit card user for storage on the card. These numbers will always be encrypted when in transmission or used in combination with transaction information, as when the card sends out transaction authorization requests (Par 72, 120; 117-130, 134-140)

Franklin discloses a electronic transaction system in which proxy credit card numbers are generated and used in authorizing merchant transactions, similar to Flitcroft, except for the fact that the "proxy" card numbers used in his system are generated at the user's end, instead of the server end (Abstract; Summary of the Invention).

Flitcroft's debit/credit card already has all the storage and computing circuitry to store limited use numbers (the claimed Cybercodes), combine them with individual transaction information, encrypt the resulting authorization requests (the claimed Cybercoupons) and then transmit these to the card issuer's central servers for authorization. It would have been obvious to one ordinarily skilled in the art at the time the invention was made to combine Flitcroft's system with Franklin's so that the Cybercodes can be generated in the cards themselves, to make the system even more convenient to users, allowing card holders to perform secure electronic transactions without need to connect to any local computer of their own. Such a combination would make the system more attractive and also more secure for of its potential customers.

As per **claim 6**.

Flitcroft in view of Franklin further discloses all the limitations of this claim (see all above citations):

...the vendor's right to give effect to said card transaction is subject to authorization by the card issuer in accordance with a method comprising:

transmitting details of the proposed transaction...;

receiving by a Filter Program ...;

discriminating by said Filter Program ...;

forwarding by said Filter Program ...;

transmitting a request which contains a Cybercoupon ...;

decrypting of said Cybercoupon ...;
replacing ...said Cybercoupon with said account number associated with said ID ...;
checking a Cybercoupon ...;
rejecting said request if said request fails any of said checks ...;
substituting, ... the relevant account number for said Cybercoupon ...;
retaining a record of all incoming requests ...,
processing of said request for authorization ...;
forwarding by the Filter Program to the vendor of said response ...;
replacing, ...with said original Cybercoupon ...;
transmitting said response ... to said vendor;
transmitting said response by the vendor to the user.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Q Le whose telephone number is 703-305-4567. The examiner can normally be reached on 8:30am-5:30pm Mo-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James P Trammell can be reached on 703-305-9768. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DQL

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600